David M. Berger (SBN 277526)
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9713
Facsimile: (510) 350-9701
dmb@classlawgroup.com

Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
Kasey Youngentob (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100 (tel.)
siegel@stuevesiegel.com
moore@stuevesiegel.com
youngentob@stuevesiegel.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OATHER MCCLUNG, ABBY LINEBERRY, TERRY MICHAEL COOK and GREG DESSART, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

ADDSHOPPERS, INC., PRESIDIO BRANDS, INC., PEET'S COFFEE, INC., and JOHN DOE COMPANIES,

Defendants.

Case No. 3:23-cv-01996-VC

PLAINTIFFS' CONSOLIDATED RESPONSE IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS

Judge: Hon. Vince Chhabria

Hearing: September 14, 2023

Time: 10:00 a.m.

Courtroom: 4

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

I. INTRODUCTION

"AddShoppers" and "SafeOpt." These names are unfamiliar to most consumers until they receive an "abandoned item" email from a retailer to whom they provided no personal information. But behind the scenes, with retailers' help, AddShoppers has built a mass surveillance enterprise called "SafeOpt." Through SafeOpt, AddShoppers runs what it calls a "Data Co-Op" that collects information about individuals from multiple sources so it can send direct advertisements on behalf of Co-Op members—taking a cut of every sale. To do this, AddShoppers installs malicious third-party tracking cookies on users' browsers and then tracks their web activity as they browse the internet, alerting it the moment the user lands on the website of one of its retail partners. Those retail partners collectively sell every imaginable good: men's health products, women's hygiene products, coffee, guns, medical supplies, and more.

And because retail partners like Every Man Jack and Peet's Coffee have installed the SafeOpt tracking software on their websites, AddShoppers knows exactly what products a potential customer viewed. This information is then added to AddShoppers' growing dossier on the unconsenting target. Worse still, AddShoppers is purportedly granted a "license" by its retail partners to use the target's personal information to send direct advertisements on behalf of "each Data Co-Op member's audience" and to "exploit" for any other purpose it deems fit. Unsurprisingly, very few individuals voluntarily opt into this program. Instead, they are unwittingly captured in it when they make a purchase or create an account on a website that—unbeknownst to them—has agreed to participate in the Co-Op.

For good reason, AddShoppers' "track and conquer" program has been universally condemned by the public. Hundreds of people have complained online about receiving targeted emails from retailers "via SafeOpt" who they never provided with their personal information. "*Creepy*", "*sleazy*", "*disgusting advertising*", "*unethical*", and an "*invasion of privacy*" are just a few snippets of the public commentary condemning this unconsented and ultra-invasive marketing practice. The arrangement also violates California law in multiple respects.

II. FACTUAL BACKGROUND

"AddShoppers runs a marketing enterprise that illicitly tracks persons across the internet, collects their personal information without consent, and then uses that information to send direct solicitations." Dkt. No. 1 (Compl.) ¶ 2. It calls this "'marketing' program 'SafeOpt.'" *Id.* ¶ 3. Most people are unwittingly brought into SafeOpt "when they create an account and make a purchase on a website that—unbeknownst to them—is part of the AddShoppers' Data Co-Op." *Id.* "AddShoppers surreptitiously collects and pools the sensitive personal information provided by individuals to online retailers in confidence, creates dossiers on those individuals, and then tracks them across the internet to monitor their web browsing for its own financial benefit." *Id.* ¶ 31.

AddShoppers does business throughout California[.]" *Id.* ¶ 10. Indeed, it partners with many California retailers including Every Man Jack and Peet's Coffee. *Id.* ¶¶ 11-12, 17. "AddShoppers also specifically advertises its alleged compliance with California's privacy laws to prospective partners." *Id.* ¶ 17. "And it sends thousands (if not millions) of targeted emails to Californians." *Id.*

AddShoppers has amassed a network with over two thousand large brands and publishers. *Id.* ¶ 26. These companies sell almost anything imaginable including "highly sensitive products." *Id.* ¶ 48. For example, people have received emails imploring them "to return to purchase a breast pump" or products "from a colon cleansing company." *Id.*

To partner with the company, AddShoppers requires participation in a "Data Co-op" which permits SafeOpt to "leverage[] a shared pool of user data collected by SafeOpt technology" by granting "SafeOpt with a limited, transferable license to their User Data for the purpose of providing identity resolution and direct messaging services for each Data Co-op member's audience." *Id.* ¶ 29. AddShoppers' terms also permit it to collect all "Client Data" derived from its partner companies, including their customers' User Data, and states that "SafeOpt may exploit Client Data for any lawful purpose without any duty of accounting or compensation to you." *Id.* ¶ 30.

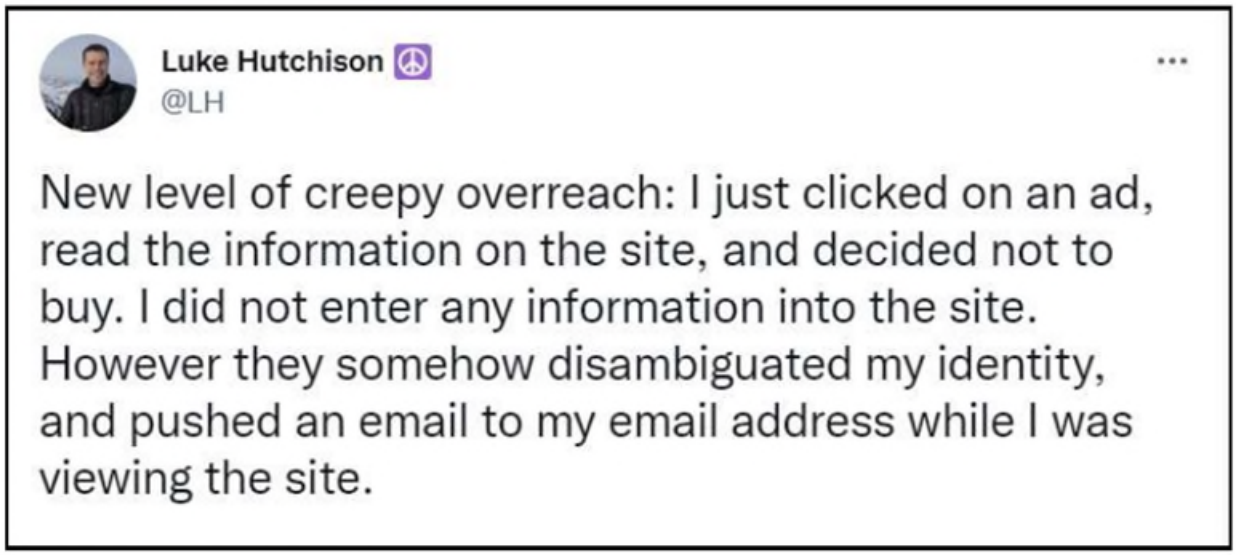
Core to AddShoppers' model is its use of "malicious, third-party tracking cookies." *Id.* ¶ 35. Retailers place this code on their website after partnering with AddShoppers—which tracks and sends information to AddShoppers about the user's browsing activity on a real-time basis. *Id.* ¶¶ 38, 41. So "[w]hen an internet user creates an account or makes a purchase with the business, a third-party tracking cookie is created that includes a unique value AddShoppers associates with that user." *Id.* ¶ 38. This cookie remains "hidden on the user's browser and automatically sends information to AddShoppers' SafeOpt domain 'shop.pe.' AddShoppers then associates that unique value with the personal information the user provided to the company, which typically includes, at a minimum, full name, address, payment card information, and email address." *Id.*

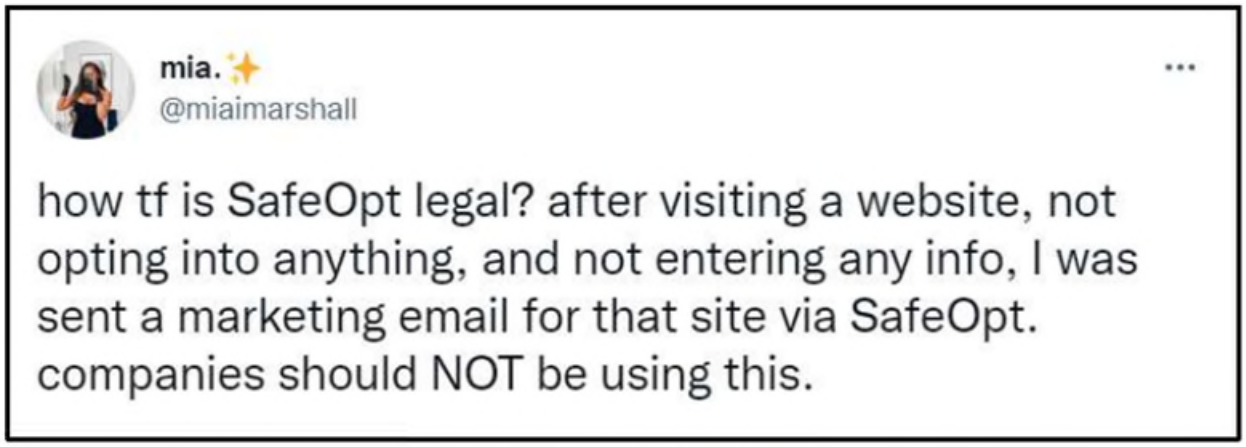
Afterward, every time a "user lands on another website in the SafeOpt network, the cookie values 'sync' and AddShoppers tracks the user's activity on the website, including the user's detailed referrer Uniform Resource Locator ('URL')." *Id.* ¶ 39. As a result, AddShoppers "can directly advertise to the user even where the user leaves a website without affirmatively providing any personal information." *Id.* Typically, it "solicits in the form of a direct email from the retailer 'via SafeOpt' imploring a user to return to the website to purchase a product they were looking at, even though the individual never gave their email address to the retailer or authorized such communications." *Id.* ¶ 43.

Plaintiffs are four such recipients—each received an email "via SafeOpt" for the exact product they had viewed on the retailer's website. *Id.* ¶¶ 59, 64, 69, 74. For example, Plaintiffs Cook and Dessart (through his wife) viewed products on the websites of California retail defendants Every Man Jack and Peet's Coffee. *Id.* ¶¶ 67, 72. Although neither Plaintiff agreed to the retailers' privacy policy nor provided any personal information, they both received an email via SafeOpt from the California retailers with the item they had viewed. *Id.* ¶¶ 67-69, 74-75.

Of course, Plaintiffs were all shocked to receive their personal browsing history from a company they never provided with their email address or any other personal information. *Id.* ¶¶60, 65, 70, 74. Plaintiffs are not alone. The Complaint includes dozens of examples of consumers complaining about receiving unsolicited direct communications from a company they did not

know was tracking their web browsing:





See, e.g., Compl. ¶¶ 45-51.

AddShoppers' Better Business Bureau webpage is also flooded with complaints. One user noted that "I received a marketing re-targeting email from a company I never gave my email to and saw it was connected to 'SafeOpt' (another purposefully misleading name to include the word 'safe'). I should have control over who has my email. It should not be possible to opt into SafeOpt's ENTIRE NETWORK OF ADVERTISERS just by opting in on ONE of them. Brands should be ashamed to use this service, it is bad for my personal data and it is bad for data security." *Id.* ¶ 46. Even after users try to opt out, "they are not actually removed from the SafeOpt network and

continue to receive marketing emails from AddShoppers. *Id.* ¶ 50-51. For instance, Plaintiff McClung, Jr. continued to receive "advertising emails from other businesses in the SafeOpt network" after he tried to unsubscribe. *Id*. ¶ 60.

"Plaintiffs each had their [personally identifiable information] PII collected by AddShoppers and their online internet browsing monitored and tracked by AddShoppers without their consent." *Id*. ¶ 76. And "[t]heir information has independent value, which is recognized by AddShoppers and members of the Data Co-Op who agree to collect and trade it for their personal gain. Plaintiffs and class members are harmed every time their PII is used or shared in a manner to which they did not consent, particularly when it is used to solicit them for marketing and advertising purposes." *Id*.

Accordingly, Plaintiffs bring nine counts: (1) violation of California Invasion of Privacy Act (CIPA), Cal. Penal Code § 631; (2) violation of the California Comprehensive Computer Data Access and Fraud Act (CDAFA), Cal. Penal Code § 502; (3) statutory larceny under California Penal Code §§ 484 & 496; (4) and (6) violation of California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code §§ 17200, *et seq*.; (7) common law trespass to chattels; (8) unjust enrichment; and (9) common law invasion of privacy.

III. LEGAL ARGUMENT

A. Legal Standard

Defendants move to dismiss under both Fed. R. Civ. P. 12(b)(1) and 12(b)(6). While under Rule 12(b)(1) plaintiffs bear the burden of proving subject-matter jurisdiction by a preponderance of the evidence, "a jurisdictional finding of genuinely disputed facts is inappropriate when the jurisdictional issue and substantive issues are so intertwined that the question of jurisdiction is dependent on the resolution of factual issues going to the merits of an action." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). And under Rule 12(b)(6), a complaint simply must contain "sufficient factual matter, accepted as true, to state a claim to relief that is *plausible* on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

B. The Court can exercise personal jurisdiction over AddShoppers[1]

The Court should apply a three-part test to decide whether the court may exercise specific jurisdiction over a non-resident defendant. Under that test: (1) "the defendant must have purposefully directed his activities at the forum . . . , thereby invoking the benefits and protections of its laws; (2) the claim must arise from or relate to the defendant's forum-related activities; and (3) the exercise of jurisdiction must comport with fair play and substantial justice (*i.e.*, be reasonable)." *S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *3 (N.D. Cal. May 15, 2019). AddShoppers' conduct satisfies this test.

1. AddShoppers purposefully directs conduct in this forum

Because Plaintiffs' claims sound in tort, the Court should apply the "purposeful direction" test for personal jurisdiction. *Picot v. Weston*, 780 F.3d 1206, 1212 (9th Cir. 2015). To purposefully direct conduct at a forum, AddShoppers must have (1) committed an intentional act, (2) expressly aimed at the forum state, that (3) caused harm that it knows is likely to be suffered in the state. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004). The allegations support purposeful direction to California.

a. AddShoppers committed an intentional act by wiretapping Plaintiffs

AddShoppers does not dispute whether it committed an intentional act. After all, that standard is "easily" met when a defendant "intentionally install[s]" a wiretap on retailer's website to purposefully intercept electronic communications. *S.D.*, 2019 WL 8333519, at *4; *see also Saleh v. Nike, Inc.*, 562 F.Supp.3d 503, 512-13 (C.D. Cal. 2021) (wiretapping satisfies the intentional act requirement). And here, "AddShoppers intentionally installed the wiretaps at issue." Compl. ¶ 16.

[1] Plaintiffs do not contest that the Court lacks general personal jurisdiction over AddShoppers.

b. AddShoppers expressly aimed conduct at California

AddShoppers expressly aimed its conduct at California in at least three ways:

First, AddShoppers placed wiretaps on "hundreds of California companies' websites" including the two Retail Defendants. Compl. ¶ 17. Those in forum partnerships show conduct expressly aimed at California. *S.D.*, 2019 WL 8333519, at *4. Neither *Saleh* nor *Massie* suggest otherwise. Instead, both cases rejected personal jurisdiction where a wiretap was allegedly installed on a *non-forum* defendant's website. *Saleh*, 562 F.Supp.3d at 514; *Massie v. General Motors Co.*, 2021 WL 2142728, at *7 (E.D. Cal. May 26, 2021).

Second, AddShoppers "specifically advertises its alleged compliance with California's privacy laws to prospective partners." Compl. ¶ 17. This too demonstrates conduct expressly aimed at California. For example, in *Will*, the Ninth Circuit held that a defendant expressly aimed its conduct at a forum where it posted webpages "on the site that address legal compliance" which were "relevant almost exclusively to viewers" in that forum. *See Will Co., v. Lee*, 47 F.4th 917, 925 (9th Cir. 2022). Here, the Complaint cites to AddShoppers' terms of service, which links to its privacy policy. *See* Compl. ¶ 28, n. 4. An entire section of that policy is dedicated to addressing California users and California law, including a "Notice to California Residents" which refers to the CCPA and California Civil Code Section 1798.83.[2]

Third, AddShoppers directly interacted with California Plaintiffs by sending them targeted emails. Compl. ¶ 59 (California Plaintiff received an email from SafeOpt); *id.* ¶ 64 (same). It also sent "thousands (if not millions) of targeted emails to Californians." Compl. ¶ 17.

In other words, AddShoppers does not passively provide software to its clients. *Cf. Massie*, 2021 WL 2142728, at *7 (court lacked personal jurisdiction where company played no role in implementing the wiretap). To the contrary, it "facilitates" its customers' "transactions with California customers." *Cf. Saleh*, 562 F.Supp.3d at 514 (cleaned up); *see id.* (Defendant software company "had no interaction with Plaintiff."). And it personally benefits from these contacts

[2] *See* https://www.safeopt.com/privacy/#notice-to-california-residents.

because "it takes a cut of all sales made 'via affiliate links in emails, texts, apps, and content.'" Compl. ¶ 43. Simply put, AddShoppers' actions go well beyond those found to avoid personal jurisdiction.

c. AddShoppers knew that harm was likely to be suffered in California

Of course, AddShoppers knew harm would occur in California. It placed wiretaps on many California businesses' websites. *Id.* ¶ 17. AddShoppers also "knew that a significant number of Californians would visit its partner websites because they form a significant portion of both companies' target market." *Id.* ¶ 16; *S.D.*, 2019 WL 8333519, at *5; *see also Will*, 47 F.4th at 927 (harm foreseeable where defendant appealed to the forum's audience).

2. Plaintiffs' claims arise from AddShoppers' forum-related activities

Plaintiffs' claims are tied to AddShoppers forum-related activities. *Id.* ¶ 16. That is, AddShoppers "alleged interception of transmission to and/or from [California]-based users—its forum-related conduct—forms the basis for the claims in the [Complaint]." *S.D.*, 2019 WL 8333519, at *5. Plaintiffs have therefore met their burden to show AddShoppers purposefully directed its conduct at the forum. *Id.*

3. The Court can reasonably exercise jurisdiction over AddShoppers

AddShoppers "must show that it would be unreasonable for this Court to exercise personal jurisdiction over it." *Id.*[3] But it offers no explanations why that would be so. The Court should reject any attempt to raise any new arguments on reply. *Gadda v. State Bar of Cal.*, 511 F.3d 933, 937 n.2 (9th Cir. 2007) ("It is well established that issues cannot be raised for the first time in a reply brief."). What's more, many courts have held it is reasonable to exercise jurisdiction over

[3] The Court should generally consider: "(1) the extent of the defendant's purposeful injection in the forum state; (2) the burden on the defendant of defending in the forum, (3) the extent of the conflict with the sovereignty of the defendant's state, (4) the forum state's interest in adjudicating the dispute, (5) the most efficient judicial resolution of the controversy, (6) the importance of the forum to the plaintiff's interest in convenient and effective relief, and (7) the existence of an alternative forum." *S.D.*, 2019 WL 8333519, at *5.

wiretapping claims. *S.D.*, 2019 WL 8333519, at *5; *Bergstein v. Parmar*, 2014 WL 12586073, at *5-6 (C.D. Cal. June 23, 2014). This is especially so when the defendant touts its compliance with California laws. *See* Compl. ¶ 17.

C. Plaintiffs have standing to pursue all their claims

To establish Article III standing, Plaintiffs must show (1) an injury, (2) that results from Defendants' conduct (3) that a court can redress. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). Defendants challenge the existence of any injury. Retail Defendants also say that none of the alleged injuries are traceable to their conduct. Both arguments lack merit.

1. Plaintiffs suffered an injury-in-fact based on privacy harms and an entitlement to unjustly earned profits

To fulfill the injury requirement, Plaintiffs must allege that they suffered a concrete and individualized violation of a legally protected interest. *In re Facebook, Inc. Internet Tracking Litig.* ("*Facebook Tracking*"), 956 F.3d 589, 598 (9th Cir. 2020). Plaintiffs "adequately allege privacy harms" to support an injury for their CIPA and privacy tort claims. *Id*. Indeed, "violations of the right to privacy have long been actionable at common law." *Id*. (cleaned up). And that right "encompasses the individual's control of information concerning his or her person." *Id*. (quotations omitted). "The California legislature intended to protect these historical privacy rights when it passed CIPA." *Id*. (cleaned up). So the "statutory provision codifies a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing." *Id*. (cleaned up). As in *Facebook Tracking*, "Plaintiffs have adequately alleged that [AddShoppers'] tracking and collection practice would cause harm or a material risk of harm to their interest in controlling their personal information."[4] 956 F.3d at 599.

Yet Defendants try to minimize Plaintiffs' privacy injury. For example, AddShoppers tries to reframe the harm as "receipt of unexpected emails." Dkt. No. 50 at 14. But Plaintiffs do not

[4] Plaintiffs agree, "unexpected emails" standing alone do not create an injury in fact. Dkt. No. 50 at 14. But here, those emails provide proof of the wiretap and real-time tracking.

contend receipt of an email alone creates injury in fact. Instead, those emails provide proof of the wiretap and illicit tracking program that underly the privacy violations alleged.

Similarly, Retail Defendants seek to reclassify the allegations as "a bare procedural violation of CIPA." Dkt. No. 51 at 13. In doing so, they incorrectly claim Plaintiffs have not plausibly alleged "that their confidential or personal information was disclosed." *Id*. But the Ninth Circuit already recognized referrer URLs—like those captured by SafeOpt—divulge "a user's personal interests, queries, and habits[.]" *Facebook Tracking*, 956 F.3d at 605. Retail Defendants shift focus on whether Plaintiffs provided their email addresses. But this ignores how the SafeOpt works: AddShoppers automatically and "*intentionally associates*" Plaintiffs' personal information with a "unique cookie value."[5] Compl. ¶ 41 (emphasis in original). And so, entering any additional personal information is unnecessary.

The allegations support this claim: "AddShoppers surreptitiously collects and pools the sensitive personal information provided by individuals to online retailers in confidence, creates dossiers on those individuals, and then tracks them across the internet to monitor their web browsing for its own financial benefit." Compl. ¶ 31; *see also id*. at ¶ 34 (AddShoppers "collects as much information relating to a user as possible all from different sources, stores that information in a centralized location where it matches data points and creates detailed profiles on individuals"). Nor can Plaintiffs realistically avoid tracking by AddShoppers' massive network which includes thousands of companies. Compl. ¶ 26. And because the network "includes companies that sell highly personal products, including feminine hygiene and men's health products," "SafeOpt can reveal exceptionally private information about customers to anyone that shares a computer." Compl. at ¶ 48 (providing examples of a breast pump and colon cleanser); *see id.* at ¶ 49 (noting

[5] AddShoppers cites the Ninth Circuit's memorandum disposition in *Cahen v. Toyota Motor Corp.*, 717 Fed. App'x 720, 724 (9th Cir. 2017). But there, Plaintiffs did "not plead sufficient facts demonstrating how the aggregate collection and storage of *non-individually* identifiable driving history and vehicle performance data cause an injury." And since then, courts have found even anonymized data collection can support standing. *Brown v. Google LLC*, --- F.Supp.3d ---, 2023 WL 5029899, at *5 (N.D. Cal. Aug. 7, 2023).

that victims have reported receiving unsolicited "emails revealing their *partner's* browsing history or had their personal browser history sent to their *work* [email] address").

Retail Defendants' reliance on *Byars* and *Lightoller* is misplaced.[6] Dkt. No. 51 at 13. Unlike here, neither case alleged pervasive tracking across the internet or unwitting participation in a "Data Co-Op" that served to the financial benefit of AddShoppers and its retail partners. Rather, those plaintiffs complained the defendants used session replay technology to capture their activities on a single website. And there was "no evidence that Plaintiff engaged in any communication with Defendant's chat feature, much less that she disclosed private information or was injured by any conduct of Defendant." *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *2 (C.D. Cal. Apr. 5, 2023); *Lightoller v. Jetblue Airways Corp.*, 2023 WL 3963823, at 8 (S.D. Cal. June 12, 2023) ("Plaintiff does not allege that she disclosed any personal information when she visited the website."). Here, the privacy harms alleged in the Complaint are even worse than *Facebook Tracking* because these Plaintiffs never knowingly registered for the service at all.

Likewise, Plaintiffs have standing to pursue their other claims. Retail Defendants insist Plaintiffs must intend to sell their personal information to establish standing. Dkt. No. 51 at 15. But "there is no constitutional requirement that Plaintiff[s] demonstrate lost economic value. Indeed, the Ninth Circuit explicitly rejected this argument in [*Facebook Tracking*], reversing the lower court's holding to the contrary." *Greenley v. Kochava, Inc.*, 2023 WL 4833466, at *4 (S.D. Cal. July 27, 2023) (citing *Facebook Tracking*, 959 F.3d at 599). "Because California law recognizes 'an entitlement to unjustly earned profits,' to establish standing, plaintiffs must only establish a stake in the profits garnered from their personal data and that it is unjust for the defendants to retain those profits." *Id*. (citing *Facebook Tracking*, 959 F.3d at 600). And Plaintiffs

[6] At any rate, both decisions may conflict with other Circuit case law. *See Garcia v. Build.com, Inc.*, 2023 WL 4535531, at *3 (S.D. Cal. July 13, 2023) ("Federal courts within California, including this Court, have held that violations of Plaintiffs' statutory rights under CIPA, without more, constitute injury in fact because unlike a bare procedural violation, a CIPA violation is a violation of privacy rights which is a more concrete and particularized harm.") (collecting cases) (cleaned up).

"seek to recover the value of the unauthorized access to their [personal information] resulting from Defendants' wrongful conduct." Compl. ¶ 77; *see Greenely*, 2023 WL 4833466, at *4 (standing met where plaintiff alleged that he conferred a benefit on the defendant through use of his personal information). Nothing more is required to show standing.

2. Plaintiffs' injuries are traceable to Retail Defendants

Both CIPA and CDAFA explicitly recognize liability for defendants that aid and abet a violation of the law. *See infra* Section III.G.1-2. And under California Penal Code § 31: All persons concerned in the commission of a crime, whether it be felony or misdemeanor, and whether they directly commit the act constituting the offense, **or aid and abet in its commission**, or not being present, **have advised and encouraged its commission, . . . are principals in any crime so committed**. (emphasis added).

Retail Defendants aided and abetted AddShoppers illegal conduct when they installed AddShoppers' wiretap on their websites. As a result, Retail Defendants are treated as principals and Plaintiffs' harms are fairly traceable to their actions. *See Vera v. O'Keefe*, 791 F.Supp.2d 959, 963-64 (S.D. Cal. 2011) (interpreting California's aiding and abetting liability under both Cal. Penal Code § 31 and CIPA); *see infra* Section. III.G.1 (discussing aiding and abetting liability).

D. Plaintiffs' claims align with state, federal, and constitutional law

AddShoppers makes a series of novel objections to all the claims. It contends Plaintiffs' interpretation of the statutes: (1) conflicts with other statutes; (2) contradicts the rule of lenity; (3) unduly burdens interstate commerce; and (4) inhibits protected speech. Dkt. No. 50 at 15-17. Each argument fails.

1. Plaintiffs' claims do not clash with the Federal Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act and the California Consumer Privacy Act (CCPA)

AddShoppers imagines a conflict between Plaintiffs' claims and certain federal or state statutes where none exists. Although CAN-SPAM and the CCPA may excuse some data collection, data sharing, or spam emails, neither allows AddShoppers' conduct here. Both statutes remain

silent on the propriety of installing a wiretap, collecting referrer URLs, and associating that information with a specific person. AddShoppers presents no case law recognizing any conflict. This Court should not be the first.

2. Plaintiffs' statutory claims do not violate the rule of lenity

AddShoppers says the rule of lenity requires the Court "avoid reinterpreting penal statutes to extend potential criminal liability." Dkt. No. 50 at 16. Even so, it highlights no ambiguity that would command its use.[7] *Wooden v. United States*, 142 S. Ct. 1063, 1075 (2022) (Kavanaugh, J. concurring) ("As this Court has often said, the rule of lenity applies only when after seizing everything from which aid can be derived, the statute is still grievously ambiguous."). Courts have therefore refused pleas to narrow either CIPA or CDAFA under the rule of lenity. *Vera*, 791 F.Supp.2d at 965 (CIPA); *Brown*, 2023 WL 5029899, at *19 (CDAFA).

3. Plaintiffs' statutory claims do not unduly burden interstate commerce

AddShoppers protests that Plaintiffs interpretation of the law "would unduly burden interstate commerce" because "any website accessible in California" could face "massive criminal liability." Dkt. No. 50 at 16. AddShoppers cites only Chief Justice Roberts' concurrence from *National Pork Producers Council v. Ross*, 143 S. Ct. 1142, 1170-72 (2023), for support. There, the Supreme Court *upheld a California law* against a Dormant Commerce Clause challenge despite complaints that it would cost pork producers $350 million to comply with the standards. *Id*. And the Ninth Circuit has rebuffed similar efforts to limit California's ability to regulate the internet using the Dormant Commerce Clause. *Greater L.A. Agency on Deafness, Inc. v. Cable News Network, Inc.*, 742 F.3d 414, 433 (9th Cir. 2014); *see also Kahn v. Outrigger Enterprises, Inc.*, 2013 WL 12136379, at *15 (C.D. Cal. Oct. 29, 2013) (refusing to dismiss CIPA claim on a motion to dismiss based on a Dormant Commerce Clause defense).

[7] AddShoppers points to a Florida state court's interpretation of the Florida Security of Communications Act. Dkt. No. 50 at 17 (citing *Jacome v. Spirit Airlines*, 2021 WL 3087860 (Fla. Cir. Ct. June 17, 2021) (Trial Order). The Florida Act has different exceptions and thus courts have repudiated attempts to read CIPA similarly. *Saleh*, 562 F. Supp. 3d at 518.

4. AddShoppers' activities are not shielded by the First Amendment

AddShoppers also invokes the First Amendment seeking to avoid liability. But it does not identify any speech rights implicated by installing a wiretap *or* implicated in tracking Plaintiffs' internet browsing. *See Maghen v. Quicken Loans, Inc.*, 2014 WL 12586447, at *5 (C.D. Cal. Oct. 28, 2014) (rejecting a First Amendment challenge to CIPA); *Vera*, 791 F.Supp.2d at 965 (same). To be sure, AddShoppers also sends emails based on those activities. But AddShoppers' illegal wiretapping is not insulated by sending an email. Accordingly, AddShoppers has not engaged in protected First Amendment speech.

E. Plaintiffs did not consent to AddShoppers' track and conquer program

The Retailer Defendants argue that Plaintiffs "consented" to the conduct here. This argument fails for three reasons: (1) the wiretap occurred before Plaintiffs could ostensibly consent; (2) Plaintiffs did not manifest assent to the Retailer Defendants' privacy polies; and (3) even if the privacy policies apply, neither policy "explicitly notified" users they were being tracked in the manner described in the Complaint.

1. The wiretap occurred before Plaintiffs could ostensibly "consent"

The Complaint alleges that companies that join AddShoppers' Data Co-Op install code on their website that automatically sends user information back to AddShoppers via a third-party tracking cookie hidden in the user's browser. Compl. ¶ 38. If the user lands on the website of another partner in the AddShoppers network, the cookie values "sync" and AddShoppers tracks the user's activity on the website, including the user's detailed referrer URL, constituting a wiretap. *Id.*, ¶ 39. Retail Defendants are members of the AddShoppers Data Co-Op and installed AddShoppers' code on their respective websites. Thus, the moment Plaintiffs landed on the Retail Defendants' websites, Plaintiffs were subjected to a wiretap before they could even ostensibly "consent" to such tracking.

In this respect, this fact pattern is similar to *Javier v. Assurance IQ, LLC*, 2022 WL 1744107 (9th Cir. May 31, 2022) (unpublished), where the panel reversed the district court's dismissal of a

class action under CIPA based on the plaintiff's "retroactive consent" of the conduct at issue. *Id*., at *1. Acknowledging the Supreme Court of California's narrow view of consent under CIPA, the panel held:

> [W]e conclude that the California Supreme Court would interpret Section 631(a) [of CIPA] to require the prior consent of all parties to a communication. Here, Javier has sufficiently alleged that he did not provide express prior consent to ActiveProspect's wiretapping of his communications with Assurance. According to the complaint, neither Assurance nor ActiveProspect asked for Javier's consent prior to his filling out the insurance questionnaire online, even though ActiveProspect was recording Javier's information as he was providing it. Javier has therefore alleged sufficient facts to plausibly state a claim that, under Section 631(a), his communications with Assurance were recorded by ActiveProspect without his valid express prior consent.

Id., at *2.

Although not precedential, the rationale of the case applies here: where a wiretap occurs *before* a user can ostensibly "consent" to the conduct at issue, consent is not a viable defense. *Cf. Javier*, 2022 WL 1744107, at *2 (Bumatay, J., concurring) ("to my knowledge, no case shows that California has adopted retroactive consent as a defense to an invasion of privacy tort.").

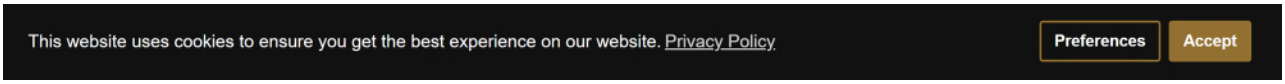
2. Plaintiffs were not on actual or constructive notice of the Retail Defendants' Terms of Service

Even if the Court determines that Plaintiffs could consent to website terms under these facts, there was no mutual manifestation of assent of the Retail Defendants' privacy policies. "Courts generally evaluate online contracts as falling into one of two categories: (1) 'clickwrap' agreements where a user is presented with the terms and conditions and must click on a button or box to indicate that he agrees before he may continue, which courts generally enforce; and (2) 'browsewrap' agreements where the website's terms and conditions are provided to users via a hyperlink at the bottom of a webpage and a user's assent to the terms is assumed by his continued use of the website, which courts often view with skepticism." *Sifuentes v. Dropbox, Inc*., 2022 WL 2673080, at *3 (N.D. Cal. June 29, 2022) (citing *Nguyen v. Barnes & Noble, Inc*., 763 F.3d 1171, 1175-77 (9th Cir. 2014)). "Browsewrap agreements are properly viewed with skepticism because

they purport to create binding contracts on terms a user is not required to review, and in the absence of any affirmative manifestation of agreement by the user." *Motley v. ContextLogic, Inc*., 2018 WL 5906079, at *2 (N.D. Cal. Nov. 9, 2018).

Here, the Retail Defendants each attempt to enforce agreements premised on virtually identical "cookie notice banners" included at the bottom of their respective websites.

Peet's:



Every Man Jack:

The cookie banners are not clickwrap agreements because they do not require acceptance of terms to use the website. They are also not traditional browsewrap agreements because they invite affirmative action by the user. *See Lopez v. Terra's Kitchen, LLC*, 331 F. Supp. 3d 1092, 1098 (S.D. Cal. 2018) ("While clickwrap agreements require the user to expressly manifest assent to the terms and conditions, browsewrap agreements do not; rather a party assents to a browsewrap agreement simply by using the website.").

Plaintiff Cook alleges that after visiting Peet's website, he clicked on and reviewed some of Peet's products but "never provided any personal information to the company, agreed to any terms on Peet's website, or clicked 'accept' on Peet's cookie acceptance banner." Compl. ¶ 67. Plaintiff Dessart never visited the Every Man Jack website at all, rather directing his wife to do so. He never alleges she accepted or even saw a cookie banner on the website. *See id.*, ¶ 72.

Although far from clear, Retail Defendants appear to argue that the privacy policy hyperlink creates a contract independent of the cookie policy and therefore should be enforced

whether or not a user clicks "accept."[8] But this argument is belied by the concept of notice. Plaintiffs did not have actual or constructive notice that by using the websites they were agreeing to the Retail Defendants' privacy policies. "[A]n enforceable contract will be found based on an inquiry notice theory only if: (1) the website provides reasonably conspicuous notice of the terms to which the consumer will be bound; and (2) the consumer takes some action, such as clicking a button or checking a box, that unambiguously manifests his or her assent to those terms." *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 856 (9th Cir. 2022).

Here, Retail Defendants cannot satisfy either prong. The banners provide that: "This website uses cookies to ensure you get the best experience on our website. Privacy Policy"—and then invite the user to click "preferences", "accept", or simply do nothing. Nowhere does the banner state that by using this website you are agreeing to a policy, instead a user must affirmatively click the hyperlink to find that out (at least for Peet's).[9] The Ninth Circuit held in *Berman* that hyperlinked text alone is insufficient to constitute conspicuous notice, even when accompanied by a disclosure that purports to requirement agreement to those terms. *See id*. at 857 ("[a] web designer must do more than simply underscore the hyperlinked text in order to ensure that it is sufficiently 'set apart' from the surrounding text.").

[8] Peet's also argues that Plaintiff Cook's allegation that he did not click accept "completely defeats all of his claims"—apparently taking the position that his acknowledgment of the banner alone is sufficient to signify acceptance of its terms (consistent with a browsewrap agreement). Opp. at 9. But it would make little sense to give a user the opportunity to "accept" terms if Peet's contends the user is bound by them regardless. In any event, even if treated as a browsewrap agreement, other courts have recognized that "cookie acceptance banners" contained at the bottom of a website are not conspicuous enough to manifest assent. *See Byars v. Goodyear Tire & Rubber Co*., 2023 WL 1788553, at *3 (C.D. Cal. Feb. 3, 2023) ("Although, the 'Terms of Use' can be found at the bottom of the webpage, Goodyear provides no argument suggesting Byars had any reason to scroll to the bottom of the webpage or otherwise saw the 'Terms of Use.'").

[9] Every Man Jack's privacy policy does not even purport to form an agreement with the website user. It states only that: "This policy describes the types of information we may collect from you or that you may provide when you visit the website everymanjack.com (our "Website") and our practices for collecting, using, maintaining, protecting, and disclosing that information." Dkt. 51-2 at 5.

There is also no unambiguous manifestation of assent. In *Berman*, the Ninth Circuit held there was no manifestation of assent even where the users clicked a large green "continue" button with smaller text underneath stating: "I understand and agree to the Terms & Conditions which includes mandatory arbitration and Privacy Policy." *Id*. at 854-57.

Here, the Plaintiffs did not click anything or take any other action that would manifest assent to the privacy policies. Just the opposite, a reasonable consumer viewing the cookie banners would likely believe that by *not* clicking "accept" they are *not* agreeing to the immediately preceding privacy policy. In the absence of affirmative conduct by Plaintiffs, there is no evidence of mutual manifestation of assent here. *Sifuentes*, 2022 WL 2673080, at *3.

3. Plaintiffs were not on actual or constructive notice of the Retail Defendants' Terms of Service

Even if Plaintiffs manifested assent to the privacy policies, they cannot serve as a valid defense to Plaintiffs' claims because they do not explicitly notify users of the conduct alleged in the Complaint. Consent "can be explicit or implied, but any consent must be actual." *Brown*, 2023 WL 5029899, at *7 (citing *In re Google RTB Consumer Privacy Litig*., 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022)). "For consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue." *Id*. In other words, "consent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct' and if the alleged tortfeasor did not exceed the scope of that consent." *Brown*, 2023 WL 5029899, at *7 (quotations omitted).

Here, the analysis can begin and end by asking two questions: First, do the Retail Defendants' privacy policies "explicitly notify" users that those who submit information to the retailer will have AddShoppers' third-party tracking cookie installed on their browser that will then track the user's activity across the internet collecting information about the user and sending it to AddShoppers to be used in a Data Co-Op involving thousands of other companies while also granting AddShoppers "with a limited, transferable license to their User Data for the purpose of providing identity resolution and direct messaging services for each Data Co-op member's

audience"? *See* Compl. ¶ 29. Second, do the policies disclose that users who visit the website but do not provide any information will have their browsing activity tracked and sent to AddShoppers so it can identify the user and cross-reference information the user has provided to other companies in the Data Co-Op so that AddShoppers can directly advertise to the user on behalf of the retailer even though the user never provided the retailer with any personal information directly?

The answer to each is a resounding "no."

In fact, neither retailer policy even mentions AddShoppers or their respective participation in the Data Co-Op. Instead, the Retail Defendants cite generalized disclosures that are at best ambiguous. For example, Peet's argues that its privacy policy discloses that cookies may be used for "tracking the pages you visit" and users are provided "targeted offers, promotions and advertising . . . via email . . . offered by Peet's or other marketing partners." Dkt. 51 at 18. But read in its broader context these disclosures refer to "preference information" sourced from pages visited *on Peet's website* and provided to "Affiliates; third party vendors and other service providers that perform website analytic services for us."[10]

Nothing in the policy discloses the nature of nature of AddShoppers' tracking beyond Peet's website or that the user's data will be shared as part of a Data Co-Op that expands far beyond Peet's affiliates and vendors. In fact, other sections of Peet's policy appear to misrepresent the extent of the data disclosure altogether. For example, Peet's represents that contact information "such as your name, billing address, shipping address, email address, telephone numbers, or other contact information" is only shared with "[o]ur affiliates and subsidiaries" and "trusted service providers." Of course, Plaintiffs allege that AddShoppers—a marketing company—regularly

[10] Another section states that targeted offers require collection of "information about you, including Usage Data and personal information such as lists of your friends, 'likes', comments you have shared, groups and location" that is sourced from "third parties, particularly social media platforms." Dkt. 51-1 at 7.

receives such information through Peet's participation in the Data Co-Op.[11]

Similarly, Every Man Jack cites to its disclosure that "We use third party advertising partners to collect information about ***your use of the Website*** in order to serve targeted advertising and to measure the performance of our advertising campaigns. The third party partners we use may collect this information using tracking technologies, such as pixels, cookies, APIs and SDKs." Dkt. 51 at 19 (emphasis added). But Every Man Jack's disclosure is limited to "use of the website"—it says nothing about tracking user's activity across other websites. Further, Every Man Jack's summary of "How We Use Your Information" omits any mention of AddShoppers or its operation of sending user information to AddShoppers in real-time to be used in a Data Co-op.

As this Court has recognized, "at this early stage of the case . . . if a reasonable [website] user could plausibly have interpreted the contract language as *not* disclosing that [defendant] would engage in particular conduct, then [defendant] cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent)." *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 789–90 (N.D. Cal. 2019) (Chhabria, J.); *see also McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *6 (N.D. Cal. Feb. 2, 2021).

At bottom, the disclosures are not limited to one plausible interpretation so Defendants cannot obtain dismissal on this basis. *See, e.g., Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 847 (N.D. Cal. 2014) (no consent to data being used for targeted advertising where users consented to its use for "data analysis"); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 824 (N.D. Cal. 2020) (consent to data collection does not extend to data disclosure); *see also Greenley*, 2023 WL 4833466, at *5 ("Even if Plaintiff gave full consent to third-party app developers to collect his data, consent to that specific conduct does not extend to Defendant's collection of Plaintiff's data through backdoors built into apps or to Defendant's dissemination of that information for profit.").

[11] Likewise, Peet's citation to users' opt-out ability carries little weight when it fails to disclose how their data is actually being used. *See Greenley*, 2023 WL 4833466, at *5 ("the failure to opt-out does not demonstrate consent, particularly when users are unaware of the data collection practices.").

4. AddShoppers Cannot Rely on the Retail Defendants' Privacy Policies

AddShoppers asserts that it "requires its clients to have privacy policies that permit AddShoppers' lawful data use" and therefore "Plaintiffs' consent to these website privacy policies bars all of their claims as to AddShoppers." Dkt. No. 50 at 22. But the Retail Defendants' privacy policies do not even comply with AddShoppers' own terms of use for its clients, which provide that its partners must "affirm that your privacy policy, your terms of service, or any other similar agreement permit you to share its 'User Data', which is the limited data collected by SafeOpt technology from the Authorized Users related to such Authorized Users' web browsing as a result of services rendered to you, ***as well as user opt-in consent to share the User Data with SafeOpt***."[12] As explained above, the Retail Defendants policies did not even mention AddShoppers or SafeOpt, let alone require "user opt-in consent to share the User Data with SafeOpt." Consequently, AddShoppers cannot win dismissal based on consent.

F. The California Retail Defendants' conduct is governed by California law

Retail Defendants contend California's statutes "under which Plaintiffs assert claims" do not govern their conduct here. Dkt. No. 51 at 16. They note CIPA generally lacks extraterritorial application. *Id*. Plaintiffs do not, however, seek any extraterritorial application of the statute because the alleged conduct occurred in California. That is, California Retail Defendants installed a wiretap on their California websites. Then, while visiting those websites, Plaintiffs' communications were collected. Courts have found CIPA governs similar interactions between non-California residents and businesses with an in-state presence like phone conversations. *See Carrese v. Yes Online Inc.*, 2016 WL 6069198, at *4 (C.D. Cal. Oct. 13, 2016) ("Thus, CIPA applies to the action, to the extent the Complaint asserts CIPA claims against a California defendant alleged for alleged conduct that occurred in California.") (collecting cases); *see also Balanzar v. Fidelity Brokerage Services, LLC*, --- F.Supp.3d ---, 2023 WL 1767011, at *8 (S.D. Cal. Feb. 3, 2023) ("It

[12] Compl. ¶ 28; *see also* SafeOpt Terms of Use Effective Date: May 12, 2021, available at https://www.safeopt.com/terms (*Id.*, n. 4).

is a reasonable inference for the Court to make that any phone call Plaintiff makes to any one of these locations in California would involve the use of the MyVoice system in the state of California."). The same should be true here.[13]

G. Plaintiffs adequately allege their statutory claims

1. AddShoppers wiretapped Plaintiffs' communications in violation of CIPA with assistance from Retail Defendants

"Though written in terms of wiretapping, Section 631(a) applies to Internet communications." *Javier*, 2022 WL 1744107, at *1 (unpublished). That provision "makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.'" *Id.* (quoting Cal. Penal Code § 631(a)). The Supreme Court of California "also emphasized that all CIPA provisions are to be interpreted in light of the broad privacy-protecting statutory purpose of CIPA." *Id.* at *2.

Plaintiffs allege AddShoppers intercepted the contents of Plaintiffs' communications, without consent, in violation of CIPA. *See Hazel v. Prudential Fin., Inc.*, 2023 WL 3933073, at *3 (N.D. Cal. June 9, 2023) (plaintiff adequately stated a claim against both the website operator and third party wiretapper). And Retail Defendants aided and abetted this violation by installing AddShoppers' wiretaps on their websites. *See, e.g., Valenzuela v. Nationwide Mutual Ins. Co.*, 2023 WL 5266033, at *6 (C.D. Cal. Aug. 14, 2023) ("Here, Valenzuela alleged that Nationwide hired Akamai specifically to intercept messages and use them for Nationwide's financial gain. Further, she alleged that Nationwide facilitated Akamai embedding Akamai's code into Nationwide's

[13] Alternatively, Plaintiffs request leave to amend California Plaintiffs' claims to allege the statutory violations against the Retail Defendants under the juridical link doctrine. *See La Mar v. H & B Novelty & Loan Co.*, 489 F.2d 461, 466 (9th Cir. 1973); *see also Akerman v. Oryx Communications, Inc.*, 609 F. Supp. 363, 375 (S.D. N.Y. 1984), *judgment aff'd and remanded*, 810 F.2d 336, (2d Cir. 1987) (refusing to certify the class because defendants were not sufficiently unified but describing what might be a sufficient juridical link: "Partnership, joint enterprise, control, conspiracy, **and aiding and abetting all may serve as such a link**, since they denote some form of activity or association on the part of the defendants that warrants imposition of joint liability against the group even though the plaintiff may have dealt primarily with a single member.") (emphasis added).

website. These are plausible allegations that Nationwide 'aided,' 'permitted,' or 'caused' Akamai's violations, which would lead to Nationwide itself being liable" under CIPA.) (cleaned up); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019) (Chhabria, J.) ("Although Moosejaw cannot be liable for eavesdropping on its own communications with Revitch, the complaint adequately alleges that Moosejaw violated section 631 by enabling NaviStone's wrongdoing."); *see also Augustine v. Lenovo (U.S.), Inc.*, 2023 WL 4938050, at *3 (S.D. Cal. Aug. 2, 2023) (denying motion to dismiss a CIPA claim where "Plaintiff alleges in the amended complaint that Quantum played an active role in recording including using the data for its own business purposes.").

Defendants do not challenge AddShoppers is an unauthorized third party or that Retail Defendants can be held liable for assisting their interception. Still Defendants argue that the CIPA claim should be dismissed for two reasons: first, they claim Plaintiffs fail to adequately plead that their communications were intercepted "in transit" in California, (Dkt. No. 50 at 17; Dkt. No. 51 at 21); and second, they assert nothing confidential was collected. Dkt. No. 51 at 22.

a. Plaintiffs' communications were intercepted while in transit in California

Plaintiffs specifically "plead an interception 'in transit' under CIPA[.]" *Hazel*, 2023 WL 3933073, at *3 (distinguishing cases). They allege "[c]ompanies that join the Co-Op agree to install AddShoppers' code on their website. When an internet user creates an account or makes a purchase with the business, a third-party tracking cookie is created that includes a unique value AddShoppers associates with that user. The cookie is hidden on the user's browser and automatically send information to AddShoppers' SafeOpt domain 'shop.pe.' AddShoppers then associates that unique value with the personal information the user provided to the company[.]" Compl. ¶ 38. Afterward, anytime a "user lands on another website in the SafeOpt network, the cookie values 'sync' and AddShoppers tracks the user's activity on the website, including the user's detailed referrer Uniform Resource Locator (URL)." *Id*. ¶ 39. As AddShoppers acknowledges, this transmission happens in "real time." *Id*. ¶ 41 (quoting AddShoppers' deleted blog post).

AddShoppers' cases dismissing CIPA provide far less detail. In *Keurig*, the plaintiff's allegations did "little more than restate the pleading requirement of real time interception." *Valenzuela v. Keurig Green Mountain, Inc.*, 2023 WL 3707181, at *5 (N.D. Cal. May 24, 2023). And in *Cinmar*, the plaintiff did not even bother naming the supposed third-party eavesdropper. *Licea v. Cinmar, LLC*, --- F.Supp.3d ---, 2023 WL 2415592, at *11 (C.D. Cal. Mar. 7, 2023); *see also id*. at *10 ("Here, Plaintiffs do not allege sufficient facts as to how and when the third party receives the communications.").[14] This case is much more similar to *Valenzuela v. Nationwide Mutual*, where the Court distinguished *Keurig* and other cases on the grounds that the plaintiff "did not simply recite that there was real time interception, she added detail on how it occurs[.]" *Valenzuela*, 2023 WL 5266033, at *5, n. 6. Plaintiffs include similar allegations here, including detailed allegations about the code installed on the retailers' websites, the operation of the third-party tracking cookies, and AddShoppers' own admission that it matches user data "*in real-time* against our network of 150M+ monthly profiles and 5,000+ websites." Compl. ¶¶ 38, 41 (emphasis added).

Plaintiffs adequately plead, moreover, that AddShoppers intercepted Plaintiff Cook and Dessart's communication in California.[15] Both Peet's and Every Man Jack are California businesses. And both California businesses installed AddShoppers' wiretap on their websites. So although Plaintiffs Cook and Dessart are located outside the state, their communications passed through California to AddShoppers.

[14] *Cinmar* is distinguishable for still another reason. There was no allegation that "the third party captured data and then used the data for its own benefit by reselling the aggregated data." *Id*. at *9.

[15] Retail Defendants argue that Plaintiff Dessart is not a party to the communication because his wife visited Every Man Jack's website. This is incorrect for two reasons. First, Plaintiff Dessart's information was captured. And second, Plaintiff Dessart's wife was acting at his direction on a shared computer. *See* Compl. ¶ 72.

b. The contents of Plaintiffs' communications were captured

Although CIPA does not speak to the nature of protected communications, Retail Defendants conceive that the communications must be "confidential." Dkt. No. 51 at 22. Plaintiffs cross even that heightened threshold. They allege AddShoppers collected their referrer URL, which allows AddShoppers to intercept and view the precise webpages and products the user is browsing. For example, Plaintiff McClung, Jr. alleges he received an email from SafeOpt including pictures of the exact firearm and ammunition he viewed. *See* Compl. ¶ 59. For good reason, courts have repeatedly held URLs contain protected information. *See Facebook Tracking*, 956 F.3d at 605 (noting that URLs divulge "a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's platform."); *see also In re Google RTB Consumer Priv. Litig.*, 2022 WL 2165489, at *10 (contents include, among other things, the "URL of the page [being visited]"; "referrer URL that caused navigation to the current page"; "details about the content within the site or app"); *Saleh*, 562 F. Supp. 3d at 518 ("customer's purchasing selections," and "interactions with" defendants' website were contents of communications).

2. Plaintiffs adequately plead a violation of the CDAFA

Under CDAFA, a person who commits any of the following acts is guilty of a public offense:

> (1) Knowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to . . . wrongfully control or obtain money, property, or data.
>
> ***
>
> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

Cal. Penal Code § 502(c)(1), (6)-(7).

Defendants contend that CDAFA's "without permission" means that "the defendant 'circumvent[ed] technical or code-based barriers in place' to prevent unauthorized access." Dkt.

No. 51 at 23 (quoting *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 950 (N.D. Cal. 2014)); Dkt. No. 50 at 19 (quoting *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1053 (N.D. Cal. 2018)). AddShoppers also argues that Plaintiffs "fail to plead damages." Dkt. No. 50 at 19. Neither argument is correct.

For starters, CDAFA's "without permission" is given its "plain meaning" and therefore "does not require the circumvention of computer barriers." *Greenley*, 2023 WL 4833466, at *14. So "[c]ode hidden in embedded software may plausibly use or take computer data 'without permission.'" *Id*. The Court should reject AddShoppers' attempt to import the Computer Fraud and Abuse Act's stricter definition. Dkt. No. 50 at 18 (citing *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012)). The Ninth Circuit has already "articulated different standards between the CDAFA and its federal counterpart and rejected the idea that, under the CDAFA, technical circumvention was necessary." *Brown*, 2023 WL 5029899, at *19 n.6 (citing *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015)).

"Because plaintiffs have alleged [AddShoppers'] knowing access to, and unpermitted taking of, plaintiffs' [browsing] activity data, they adequately state a claim under the CDAFA." *Rodriguez v. Google LLC*, 2021 WL 2026726, at *7 (N.D. Cal. May 21, 2021). Like their CIPA claim, Plaintiffs have adequately pleaded Retail Defendants assisted AddShoppers' CDAFA violation. *COR Sec. Holdings Inc. v. Banc of California, N.A.*, 2018 WL 4860032, at *7-8 (C.D. Cal. Feb. 12, 2018) (recognizing aiding and abetting liability).

Plaintiffs also adequately plead damages. *Facebook Tracking* "stands for the proposition that plaintiffs can state an economic injury for their misappropriated data." *Brown*, 2023 WL 5029899, at *19. And Plaintiffs allege that "AddShoppers' appropriation of class members' PII was to its economic and commercial advantage." Compl. ¶ 128. Given that AddShoppers claims a "license" over their information, Plaintiffs further allege they are entitled to the value of the unauthorized access to their PII resulting from Defendants' wrongful conduct, which can be measured using damages theories analogous to the remedies for unauthorized use of intellectual property (*i.e.*, a "reasonable royalty" from an infringer). *Id*. ¶ 77.

3. Plaintiffs adequately plead a UCL claim

"The UCL provides a cause of action for business practices that are (1) unlawful, (2) unfair, or (3) fraudulent." *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 636 (N.D. Cal. 2021). Plaintiffs allege that AddShoppers and John Doe Companies violated the first two prongs of the UCL. First, Plaintiffs allege that AddShoppers and John Doe Companies engaged in unlawful practices by violating state statutes like CIPA, CDAFA, and statutory larceny. *Id*. Second, Plaintiffs allege that AddShoppers and John Doe Companies engaged in unfair practices, including violating state statutes. *Id*. AddShoppers argues that Plaintiffs lack an economic injury because they have not lost money or property. Dkt. No. 50 at 19-20; Dkt. No. 51 at 23.

But the case law now holds that the use of personal information without consent constitutes economic injury. *See Brown*, 2023 WL 5029899; *Klein v. Facebook, Inc.*, 580 F. Supp. 3d 743, 803 (N.D. Cal. 2022) ("numerous courts have recognized that plaintiffs who lose personal information have suffered an economic injury"); *Calhoun*, 526 F.Supp.3d at 605 (collecting cases). Here, Plaintiffs allege Defendants "stole, took, or fraudulently appropriated Plaintiffs' PII without their consent." Compl. ¶ 119. And that "[b]y selling or providing personal information and data without consent . . . AddShoppers engaged in unlawful and unfair acts and practices." *Id*. ¶ 126. Further, "Plaintiffs would not have purchased from John Doe Companies if they had known they would be placed into SafeOpt." Compl. ¶ 153. Said differently, Plaintiffs lost the benefit of their bargain in their purchases from the John Doe Company that opted them into the surveillance network. And "[c]ourts in California have consistently held that benefit of the bargain damages represents economic injury for purposes of UCL." *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 2020 WL 2214152, at *9 (S.D. May 7, 2020).

4. Plaintiffs adequately plead a statutory larceny claim

"California Penal Code Section 484 forbids theft, which includes obtaining property 'by . . . false . . . representation or pretense.'" *Calhoun*, 526 F.Supp.3d at 635. And "California Penal Code Section 496(a) prohibits the obtaining of property 'in any manner constituting theft.'" *Id*.

Here, Plaintiffs "allege that [AddShoppers] violated these sections by stealing Plaintiffs' personal information without Plaintiffs' consent." *Id*.; Compl. ¶ 119. Retail Defendants are also liable under California Penal Code § 31 which treats them as principals because they aided and abetted AddShoppers' statutory larceny. Compl. ¶ 117. While Defendants contend that personal information does not equate to property for statutory larceny, "California courts have . . . acknowledged that users have a property interest in their personal information. *Calhoun*, 526 F.Supp.3d at 635 (collecting cases). This is especially true because AddShoppers claims a "license" over Plaintiffs' personal information to "exploit" for any purpose it chooses. *See* Compl. ¶ 29-30.

H. Plaintiffs adequately plead their common-law claims

1. Plaintiffs adequately plead a privacy tort claim

To state a claim for intrusion upon seclusion, Plaintiffs must plead: (1) "a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Facebook Tracking*, 956 F.3d at 601. Plaintiffs satisfy ever element here.

a. Plaintiffs had a reasonable expectation of privacy against AddShoppers' tracking

Plaintiffs have an objectively reasonable expectation of having their private internet browsing activity remain private. California courts have recognized that such an expectation exists "over URLs that disclose either unique 'search terms' or the 'particular document within a website that a person views.'" *Brown*, 2023 WL 5029899, at *20 (quoting *Hammerling v. Google LLC*, 615 F.Supp.3d 1069, 1089 (N.D. Cal. 2022)); *see also Rodriguez v. Google LLC*, 2021 WL 2026726, at *8 (N.D. Cal. May 21, 2021) (noting reasonable expectation of privacy in, among other things, "detailed URL requests."). AddShoppers, assisted by Retail Defendants, surreptitiously captures that very information. Compl. ¶ 2. As a result, Plaintiffs have a reasonable expectation of privacy.

b. AddShoppers' intrusion was highly offensive

To decide "whether a defendant's actions were highly offensive to a reasonable person," the Court should consider "factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing

interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606 (quotations omitted). "For this reason, courts hesitate to decide the issue at the pleading stage." *Greenley*, 2023 WL 4833466, at *12 (citing *Facebook Tracking*, 956 F.3d at 606).

Defendants try to cast their action as "routine commercial behavior." Dkt. No. 50 at 20. But the public's response reveals otherwise. Compl. ¶ 45 (collecting just "a small sample of user complaints" including tweet stating, "Ever browse a product on a site, but don't even add it to your cart or enter your email ... And then get a sales email moments later? It's called SafeOpt. And I absolutely hate it. Feels so invasive -- just me?"); *see id.* ¶ 46 (noting "AddShoppers' Better Business Bureau webpage is also flooded with complaints"). Nor has any court held that the pervasive level of surveillance AddShoppers engages in is not highly offensive. *See Revitch*, 2019 WL 5485330, at *3 ("A jury could conclude that this intrusion, which allegedly allowed NaviStone to associate Revitch's browsing habits with his identity, is a highly offensive breach of norms."). Defendants are left with pre-*Facebook Tracking* authority, most a decade old, and whose facts bear little resemblance to this case. *See In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (disclosure of Google data only); *Low v. LinkedIn Corp*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (disclosure of users' LinkedIn profile viewing history only); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011), *as modified* (June 7, 2011) (collection only of plaintiff's address).

2. Plaintiffs adequately plead a standalone unjust enrichment claim

"To allege unjust enrichment as an independent cause of action, a plaintiff must show that the defendant received and unjustly retained a benefit at the plaintiff's expense." *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016). Here, AddShoppers received and unjustly retained a benefit at Plaintiffs' expense when it wrongfully collected and exploited their personal data for commercial gain. *See Lundy v. Facebook Inc.*, 2021 WL 4503071 (N.D. Cal. Sept. 30, 2021); *Hart v. TWC Prod. & Tech. LLC*, 2021 WL 1032354, at *8 (N.D. Cal. Mar. 17, 2021) ("Even though the Court earlier concluded that Hart 'suffered no economic loss from the

disclosure of [his] information, [he] may proceed at this stage on a claim for unjust enrichment to recover the gains that [TWC] realized from its allegedly improper conduct.'" (citation omitted)).

And contrary to AddShoppers argument, Plaintiffs need not show that they "'directly expended their own resources'" or "'that their property has become less valuable.'" Dkt. No. 50 at 22 (quoting *Katz-Lacabe v. Oracle Am., Inc.*, --- F.Supp.3d ---, 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023)); *see Facebook Tracking*, 956 F.3d at 599 (recognizing "a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss"). This is textbook unjust enrichment as each Defendant financially benefited from its participation in the AddShoppers Data Co-Op at the expense of Plaintiffs and class members.

AddShoppers also asserts that unjust enrichment is not a standalone claim under California law. "[T]hat argument is based on outdated law." *See Brooks v. Thomson Reuters Corp.*, 2021 WL 3621837, at *11 (N.D. Cal. Aug. 16, 2021); *see also Rojas v. Bosch Solar Energy Corp.*, 443 F. Supp. 3d 1060, 1080 (N.D. Cal. 2020) (recognizing unjust enrichment as a standalone claim); *Wu v. Sunrider Corp.*, 2017 WL 6880087, at *4 (C.D. Cal. 2017) (same).

IV. CONCLUSION[16]

Plaintiffs respectfully request that the Court should deny Defendants' motions to dismiss in their entirety, but that any dismissal, in whole or in part, should be without prejudice and with leave to amend.

[16] Plaintiffs agree to voluntarily dismiss their trespass to chattels claim pending further discovery as to whether AddShoppers' cookies interfered with and impeded Plaintiffs' use of their computers.

Dated: August 17, 2023

Respectfully submitted,

/s/ *Norman E. Siegel*
Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
Kasey Youngentob (*pro hac vice*)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100 (tel.)
siegel@stuevesiegel.com
moore@stuevesiegel.com
youngentob@stuevesiegel.com

David M. Berger (SBN 277526)
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9713
Facsimile: (510) 350-9701
dmb@classlawgroup.com